



XLIX Legislatura

**DEPARTAMENTO
PROCESADORA DE DOCUMENTOS**

Nº 779 de 2021

Carpeta Nº 1734 de 2021

Comisión Especial de innovación, ciencia y tecnología

TIPIFICACIÓN DE CIBERDELITO

Normas

MINISTERIO DE EDUCACIÓN Y CULTURA
Y PLAN CEIBAL

Versión taquigráfica de la reunión realizada
el día 18 de noviembre de 2021

(Sin corregir)

Preside: Señor Representante Gustavo Olmos.

Miembros: Señores Representantes Sebastián Cal, Miguel Lorenzoni, Martín Melazzi, Raúl Vilacoba y señora Representante Dayana Pérez.

Asiste: Señor Representante Rafael Menéndez Cabrera.

Invitados: En representación del Ministerio de Educación y Cultura, doctor Gastón Gianero, Director de Asuntos Constitucionales, Legales y Registrales y por el Plan Ceibal, Magister Leandro Folgar, Presidente.

Secretarias: Señoras Myriam Lima y Margarita Garcés.

═══════II═══════

SEÑOR PRESIDENTE (Gustavo Olmos).- Habiendo número, está abierta la reunión.

Dese cuenta de los asuntos entrados.

(Se lee:

EL BANCO CENTRAL DEL URUGUAY. Remite información en relación a una nota de prensa publicada en la página web del grupo multimedio bajo el título "Aumentó el 25 por ciento el ciberdelito en los dos últimos años." Asunto Nº 153166).

——Es un gusto recibir al doctor Gastón Gianero, director de Asuntos Constitucionales, Legales y Registrales del Ministerio de Educación y Cultura y al magíster Leandro Folgar, presidente del Plan Ceibal.

La Comisión tiene a consideración el proyecto de ley relativo a "Tipificación de ciberdelitos". En ese marco, estamos recibiendo a instituciones, organismos públicos y privados que nos parece que pueden brindar aportes.

SEÑOR FOLGAR (Leandro).- Buenos días. Es un gusto saludarlos.

Primero que nada quiero decir que celebramos esta iniciativa. Desde el Plan Ceibal vemos muy bien que se esté discutiendo este tema tan complejo y que se esté tratando de encontrar instrumentos que nos ayuden a regularlo y ordenarlo.

Por otra parte, procuraremos presentarles hoy la amplia complejidad -que entendemos ya conocen- que tiene este asunto, que también tiene oportunidades hacia adelante, que vamos a comentar.

Voy a referirme a algunos puntos asociados a las realidades que tenemos que enfrentar, en concreto, desde Ceibal y a las estrategias que estamos tomando proactivamente en la educación respecto a esta cuestión. Luego, el doctor Gastón Gianero se va a referir a los aspectos legales y jurídicos, que me exceden.

Traje una pequeña presentación para mostrarles.

La intención es hablar de los ciberataques en el marco de los riesgos globales; de la ciberseguridad en educación; de los efectos covid- 19; hacer comentarios respecto al proyecto -que veíamos en concreto en aplicaciones para educación- y referirnos a la educación en ciberseguridad dentro de lo que es el proyecto de Ciudadanía Digital, que están impulsando tanto el Plan Ceibal como la ANEP.

No sé si han visto la matriz que está en pantalla. El World Economic Forum publica esta matriz, en la que muestra qué tan probables son ciertos riesgos y qué impacto podrían tener. Ciberseguridad o ataques de ciberseguridad es el único punto violeta que se encuentra en el cuadrante derecho superior; lo aclaro porque no espero que nadie pueda leer lo que dice en la presentación, ya que ni siquiera yo lo leo en la pantalla de la computadora. Eso habla de que esta es de las cuestiones más probables que sucedan y que pueden tener más impacto a nivel de las organizaciones y a nivel económico dentro de cualquier emprendimiento.

SEÑOR PRESIDENTE.- ¿Qué tenemos en los ejes X e Y?

SEÑOR FOLGAR (Leandro).- En el eje de la X está la probabilidad de que suceda y en el de la Y -en las ordenadas-, el posible impacto.

Luego, les voy a compartir esta presentación; la traje en *pendrive* para dejárselas.

El punto verde que está más arriba y a la derecha refiere a cuestiones asociadas al cambio climático. El punto rojo que ven más arriba -que no estaba ahí, no existía; nadie lo tenía previsto- tiene que ver con las enfermedades infecciones y pandemias. Así que esa matriz ha ido cambiando mundialmente.

En cuanto a los riesgos corporativos, KPMG lanza una encuesta con resultados bastante interesantes. Esta es la percepción de los CEO -de los gerentes generales dentro de las organizaciones- respecto a cuáles son los riesgos más grandes y que menos posibilidades de controlar tienen desde su lugar. Los riesgos de ciberseguridad están al tope de la escala. En la presentación esto también se ve algo chico, pero los riesgos de seguridad son una de las percepciones mayores dentro de los riesgos a mitigar de parte de los CEO de las organizaciones.

En cuanto al *top* de ciberamenazas durante la pandemia, el último reporte de Interpol refiere a los cuatro ciberdelitos más frecuentes: la estafa de fraude o *phishing,* que es capturar información de otros por cualquier medio tecnológico; la instalación de *software* malicioso en computadoras -*malware, ransomware*- ; los dominios, las direcciones web que puedan ser maliciosas -que representan un 22 %- y las noticias falsas, con un 14 %.

En cuanto a educación -en este punto, vamos a hablar de lo que nos ha tocado a nosotros enfrentar-, obviamente, por la acción del covid- 19, la virtualidad o el tiempo que se pasaba dentro de las plataformas educativas y de medios digitales se incrementó muchísimo así como la cantidad de información que volcaban nuestros docentes y estudiantes en esos espacios.

A esto se sumaron fenómenos que no se daban: que estas plataformas fueran pasibles de ciberataques por parte de organizaciones internacionales con el objetivo de ganar palanca, de ganar información que después pudieran utilizar para otros fines. Este es uno de los riesgos más grandes y en lo que tiene que ver con ciberdelitos, es de los que más está creciendo.

Para que se hagan una idea, hoy existen productos de aseguradoras en todo el mundo que tienen que ver con seguros para ciberataques. Esto obedece a que para una empresa es más barato reputacionalmente pagar un rescate que asumir que recibió un ciberataque, que la información de su compañía ha sido sustraída y que los datos de sus clientes pueden estar en manos de personas que, después, quieran utilizarlos a favor de actividades delictivas.

Aquí es cuando empieza a ramificarse una de las complejidades.

El proyecto articula muy bien muchos de los delitos que están asociados a personas individuales, pero también tenemos un riesgo adicional asociado a lo que tiene que ver con las instituciones y a su vez, con cómo esas estafas a personas individuales pueden incidir en estos otros delitos. Ahí, los ciberdelincuentes han encontrado un nicho de mercado. Y lo cierto es que es un mercado rentable. ¿Por qué? Porque las organizaciones financieras, las aseguradoras se han dado cuenta de que es mejor tener seguros, pagar rescates y demás -si son de determinados montos- y evitar los riesgos reputacionales. En consecuencia, en muchos casos las empresas aseguradoras están exigiendo a sus asegurados determinados niveles de seguridad y protocolos de seguridad. |En ese sentido, este es un desafío para la unidad de ciberdelito que pueda tener Uruguay. Me refiero, por ejemplo, a cómo vincularse con esas divisiones de las empresas aseguradoras.

En educación, tenemos el mandato adicional de tener que proteger esa información, entre otras cosas, porque son interacciones entre adultos y menores en el entorno de un ámbito educativo: docentes y estudiantes, a partir de Ceibal, en las plataformas.

Nosotros, lo que garantizamos es que lo que esté pasando allí sea una extensión del aula y que esas interacciones estén reguladas con los mismos protocolos con los que las regula la ANEP. Para eso, tenemos una comisión de ciberseguridad que se ha creado en Ceibal hace ya un tiempo, que ha ido mejorando e incrementando las medidas de seguridad tanto para docentes como para estudiantes.

Ustedes recordarán que el año pasado hubo algunos episodios vinculados al nivel de inseguridad de las contraseñas de algunos de los actores que estaban utilizando las plataformas y los problemas de suplantación de identidad que eso podía ocasionar.

¿Qué acciones tomamos? Tomamos acciones que tienen que ver con la certificación de calidad en ciberseguridad desde Ceibal en todos los protocolos a la interna de la organización y a su vez, en los servicios que brindamos. Además, tomamos los recaudos de formar esta comisión de ciberseguridad, que está todo el tiempo no solo revisando, sino capacitando a todo nuestro personal en cuanto a cómo hacer un uso apropiado de estos medios.

Después, tenemos una línea relativa al servicio que brindamos y al compromiso social que tenemos, que tiene que ver con la parte educativa en ciudadanía digital. En este sentido, procuramos tener un enfoque integral desde la ciudadanía digital, en cuanto a desarrollar competencias para ejercerla de manera responsable. Nos enfocamos, por un lado, en el uso crítico y reflexivo y por otro, en el uso creativo y participativo.

Entendemos que no existe una división entre el mundo virtual y el mundo real, sino que hay un único mundo que se expresa por medios diferentes.

El otro día, un adolescente me decía -me pareció sumamente emblemático- : "Muchos adultos todavía piensan que mis amistades por internet son un poco menos reales de lo que ellos creen". Lo cierto es que no necesariamente estamos preparados para estas generaciones que, cuando ciertos vínculos que se dan por medios virtuales cumplen ciertas condiciones, consideran que tienen el mismo valor que el que nosotros podíamos percibir en lo que llamamos la realidad real.

La realidad real es una gran realidad que tiene expresiones en lo virtual, en lo digital y en el mundo físico, y ha evolucionado; estamos aumentados en ese sentido, y por eso es tan desafiante.

Desde Ceibal, con la línea de Ciudadanía Digital procuramos, básicamente -y a partir de lo que nos ha tocado vivir-, analizar cómo se ve el ejercicio de la democracia en medios digitales en un mundo pospandemia y cómo podemos formar con esos fines.

En ese sentido, el proyecto nos da un marco, pero también nos plante desafíos en cuanto a que cada uno de los ciberdelitos o de los delitos que conocemos -en el entendido de que la realidad es una sola y se expresa por múltiples medios- se puede manifestar por medios virtuales o digitales. Eso implica que, tal vez, haya que mirar el Código Penal como un todo, teniendo en cuenta que cada uno de los delitos puede tener su expresión en el ámbito digital o virtual.

Las competencias para el uso seguro y responsable que estamos promoviendo tienen que ver con la autorregulación, con el comportamiento ético, con el comportamiento empático, con conocer y ejercer los derechos en el entorno digital, con la conciencia de la huella digital, con la construcción de la identidad digital y con el manejo de la privacidad y de los riesgos. Esas son las áreas en las que entendemos que, desde edades tempranas, tenemos oportunidad de hacer diferencia.

Tal vez, una de las áreas más importantes sea la conciencia de la huella digital y de que mi identidad -si entendemos que la realidad es una gran realidad que se expresa por

múltiples medios-, es mucho más integral y se expresa por múltiples medios, si así lo decido: se expresa en el medio digital y en el ámbito virtual, también.

Dejo por aquí la presentación inicial y cedo el uso de la palabra a Gastón para que hable del proyecto.

Les consulto si tienen alguna pregunta específica sobre esto y les reitero que les voy a entregar copia de esta presentación.

SEÑOR PRESIDENTE.- Muchas gracias.

La idea es que ustedes expongan y luego, hacemos una ronda de preguntas.

Así que puede intervenir el doctor Gianero.

SEÑOR GIANERO (Gastón).- Muchas gracias.

Es un gusto, como siempre, estar acá. También es una responsabilidad ser invitado y que, de alguna manera, nuestra opinión pueda colaborar en la tarea que tienen a su cargo.

En primer lugar, quiero señalar la importancia que tiene que los legisladores hayan tenido la iniciativa de tomar este tema, colocarlo en la agenda, analizarlo y hasta formular propuestas concretas.

En la línea de lo que venía diciendo el magíster Folgar, en materia de ciberdelincuencia uno puede imaginar tres conceptos que podrían ser denominados como ciberdelitos.

Por un lado, está el concepto de ciberdelito aludiendo al medio por el cual se comete o se realiza la conducta penalmente reprochable.

El ciberdelito también puede ser el concepto de aquella conducta que, únicamente, puede ser desarrollada o que tiene características especiales cuando es desarrollada por medios digitales o tecnológicos -les pido disculpas, pero, por mi edad, voy a utilizar los términos mucho peor que el magíster Folgar; ustedes sabrán comprender nuestra brecha generacional-, cuya reprochabilidad penal deviene de las características especiales que en ese medio tiene o de las consecuencias que tiene el cometer esas conductas por un medio digital.

Finalmente, un tercer concepto de ciberdelito es que es aquel que hace al ataque a la ciberseguridad o el ciberataque.

Es bueno separar los conceptos porque nos puede llevar a tratamientos distintos.

Cuando hablamos del ciberdelito como medio para cometer la conducta ilícita, debemos ser precisos. Si condeno una determinada conducta y la califico como ciberdelito cuando únicamente estoy hablando del medio por el cual se comete la conducta, puedo estar dando la pauta -en términos de ordenamiento jurídico- de que otras conductas que no tengan la previsión expresa del medio tecnológico o digital como medio de cometer la conducta, no deben ser sancionadas.

Nosotros podemos hablar de la estafa y decir: "El que mediante engaños o estratagemas artificiosas…". En realidad, la estafa es un tipo delictivo que no tiene ninguna característica excluyente del medio digital o tecnológico para ser cometida. El engaño o la estratagema artificiosa perfectamente pueden ser llevarse a cabo de manera personal, telefónica, por medio telemático o digital. En realidad -auque no soy yo el que legisla; son ustedes-, no sé si merece un tratamiento específico cuando estoy hablando del medio por el cual se comete la conducta. Puedo estar dando la pauta de que otro delito al que no le doy la expresión a partir del medio por el cual se comete, si es por medio digital, no constituye conducta penalmente incriminable.

Espero haber expresado claramente esta idea.

Distinto es el ciberdelito cuando lo conceptualizamos como aquel que solo puede desarrollarse por medio digital o tecnológico o adquiere ribetes o consecuencias especialmente dañinas, que ameritan la condena del Estado. Un ejemplo claro es lo que se denomina *stalking*, que está previsto en el proyecto. Claramente, el acoso por medio digital o tecnológico no es que solo se pueda acosar por medio digital, pero adquiere una trascendencia y genera una consecuencia en el sujeto pasivo que, evidentemente, lo hace merecedor de una tipificación penal específica.

En tercer lugar, está la ciberseguridad que a nosotros -los más grandes- nos obliga a reformular cuestiones que tenemos demasiado arraigadas en lo que hace al Derecho Penal. A un señor mayor como yo, se le hace difícil concebir un tipo delictivo carente de sujeto pasivo. ¿Cómo puede ser que haya un tipo delictivo sin sujeto pasivo, ya sea este persona física, jurídica o el Estado? ¡Alguien tiene que haber enfrente! Sin embargo, en el ciberdelito o en la ciberseguridad, el sujeto pasivo de la eventual conducta penalmente reprochable es un sistema informático; es una construcción sin personas.

Cuando yo hablo de la estafa, por ejemplo, puedo referirme a la estafa como ciberdelito. Personalmente, entiendo que la estafa ya está incluida en el tipo delictivo actual, cuando se produce por medio digital. Sin embargo, nos seguimos refiriendo a estafa como aquel que "indujere a error a alguna persona para procurar […]". Es decir: yo estafo al sistema informático, a las vallas, a las puertas, a los códigos, a lo que sea que me impida -de acuerdo con el desarrollador- acceder a lo que yo quiero.

Entonces, no es suficiente aquella vieja enseñanza que nosotros teníamos en la que había sujeto activo, sujeto pasivo, verbo típico, condiciones de punibilidad; no es suficiente aquel esquema del Derecho Penal que uno aprendió para empezar a castigar a este tipo de conductas.

Digo esto en términos generales.

Desde el año 2001, tenemos el Convenio Sobre la Ciberdelincuencia, de Budapest. Efectivamente, el proyecto reconoce este Convenio; de alguna manera, es el inspirador o el que está detrás. Lo que no surge es la razón -debe haberla- de por qué no se ha caminado hacia la ratificación de este Convenio

Este Convenio -que tiene algunos aspectos que son opinables-, nos habla de las herramientas de cooperación jurídica internacional. Así como nuestro ordenamiento jurídico penal, eventualmente, deja fuera a alguna de las conductas que a partir del desarrollo digital o tecnológico han adquirido ribetes penalmente recriminables, el ámbito procesal también debe adaptarse a los tiempos que nos genera la persecución, la investigación o la represión de los ciberdelitos. No es imaginable que el trámite de un exhorto o de una carta rogatoria a través de las autoridades centrales, de los ministerios de relaciones exteriores de distintos países o de la vía diplomática o consular, sea la respuesta adecuada para la protección de pruebas, ingresos y respaldos que puedan estar en servidores; no quiero meterme con conceptos tecnológicos porque voy a meter la pata. Me refiero, por ejemplo, a cuáles fueron las comunicaciones mantenidas, qué contenido tuvieron esas comunicaciones, si efectivamente existieron, etcétera. Eso hay que protegerlo, inmovilizarlo y evitar su pérdida en forma lo suficientemente inmediata como para que sea efectiva. Se trata de una forma tan inmediata que las actuales herramientas de cooperación jurídica internacional no nos lo permitirían.

Además, hay otra cuestión, que es la opinable en el Convenio de Budapest, pero que nos permite poner el tema sobre la mesa: la jurisdicción. Si nosotros conceptualizáramos la ciberdelincuencia como un delito más, estaríamos perdiendo de vista que es el delito por

excelencia que tiene una extraterritorialidad absoluta, no solamente en materia penal, sino también en materia turística; digo esto con propiedad porque hace muchos años supe ser director de jurídica del Ministerio de Turismo.

El tema es definir dónde se comete la conducta ilícita. ¿Se comete dónde está sentado el señor sujeto activo de la misma? ¿En la nacionalidad del servidor por el cual se conecta? ¿En la nacionalidad o el lugar físico donde se encuentra la víctima, en caso de haberla? En caso de que la víctima o el sujeto pasivo no sean un sujeto, sino una red, ¿cuál sería la jurisdicción que puedo llegar a aplicar?

El Convenio de Budapest genera algún problema en este sentido. No sé si no deberíamos -tal vez no sea yo el indicado; debe ser gente más experta en la materia- bajar esto a tierra y pensarlo. Sin embargo, me parece que tendría que ser un complemento necesario de un proyecto de ley sobre el ciberdelito definir la jurisdicción aplicable y cómo se determina esa jurisdicción competente para dilucidar las cuestiones vinculadas al ciberdelito.

El Convenio de Budapest -más allá de que, insisto, tiene algunas dificultades- fue ratificado por sesenta países. Voy a demostrar el poco conocimiento y desarrollo digital e informático que tengo al agregar que muchos de esos países son de la región. Parecería que este fuera un hecho importante, pero no lo es. En ciberdelito eso no importa. En materia de ciberdelito es tan importante que lo haya ratificado Argentina como que lo haya ratificado Australia, porque esa es la característica del ciberdelito: la extraterritorialidad. En definitiva, sesenta países lo han ratificado, fundamentalmente, en lo que hace a la herramienta jurídica internacional. Este es un motivo que sugiere la reflexión.

Les consulto si quieren que analice cada uno de los artículos propuestos.

SEÑOR PRESIDENTE.- Quiero hacer una aclaración.

El Convenio de Budapest está en trámite en el Poder Ejecutivo. Está en la etapa de presentación de informes de los ministerios competentes para, luego, ingresar al tratamiento parlamentario. Nos han dicho que ingresaría al Parlamento en las próximas semanas. Somos absolutamente conscientes de que es un paquete.

Por otra parte, creo que sería mejor que el doctor Gianero analizara cada uno de los artículos y después, pasar a las preguntas de los diputados y diputadas.

SEÑOR GIANERO (Gastón).- Gracias por la aclaración. Pido disculpas porque no lo sabía.

Se propone como artículo 1º el agregado del inciso segundo del artículo 288. Dado que una de las principales reglas de interpretación de las normas es su tenor literal, la inclusión de anglicismos o expresiones en idioma extranjero nos podría llegar a generar algún problema. No estoy en la discusión de soberanía de la lengua; no es ese el punto. El punto es no ser los dueños, como país, de darle el contenido a la expresión incluida en la norma. Yo sé que es el tipo delictivo desarrollado, no el *nomen iuris,* el que determina cuál es la conducta penalmente recriminable.

Ahora bien, o llego a la conclusión de que el *nomen iuris* no me sirve para nada, o puedo advertir, eventualmente, la inclusión de anglicismos. Insisto que no es un tema de soberanía del idioma, porque hay anglicismos que están absolutamente incorporados y no hay forma de designar lo que el anglicismo o neologismo designa. Nadie va a discutir que la pizza debe llamarse pizza*,* y no sabríamos cómo llamarla si no utilizáramos ese neologismo, pero con *stalking* o *grooming* no sucede lo mismo. Esta es una opinión personal y, por supuesto, serán ustedes quienes lo definan.

En el artículo 2º del proyecto -273 inciso 4- se incluye: "[…] o bien le muestre imágenes pornográficas en las que se represente o aparezca un menor de edad […]". ¿Y por qué no un mayor de edad también? ¿Cuál es el motivo por el que excluimos, como conducta penalmente reprochable, la exhibición de imágenes pornográficas de mayores de edad al menor? Es simplemente una apreciación.

Con respecto al artículo 3º, que refiere a la estafa informática, me remito a lo que había señalado. Si lo definimos o lo circunscribimos a que el destinatario de la conducta sea alguna persona, dudo de la necesidad de la inclusión del artículo, porque claramente encuadra en la estratagema o engaño artificioso previsto en el artículo 347 actual. Me parece perfecto que se haga una descripción más ampliada en los literales A, B y C contenidos en el artículo, pero sugeriría aprovechar la oportunidad para eliminar "alguna persona" e incluir la estafa a la barrera, al sistema, a la construcción informática. Esta es una mera sugerencia; son aportes que pueden ser compartibles o no. Es lo que a uno le ha llamado la atención del proyecto, y lo digo con sumo respeto y delicadeza.

Con respecto al artículo 4º que refiere a daños informáticos, no digo que esté de acuerdo o en desacuerdo. Son conscientes y tendrán sus razones la Comisión, los proponentes del proyecto y, eventualmente, las Cámaras cuando lo aprueben, del mantenimiento de una adecuada dosimetría penal. Es decir, lo estamos condenando, con este guarismo de condena que es distinto a otros, queriendo que así sea. Se nos ha señalado -lo digo como operador jurídico- que en algún caso no estamos manteniendo una adecuada dosimetría penal. No estoy hablando puntualmente de este artículo, sino de que en términos generales tenemos la tendencia social, humana, razonable, de que cuando una conducta adquiere ribetes de especialmente reprochable, ya sea por la difusión o por las consecuencias que en ese momento y en ese lugar genera, la castigamos con una dimensión que tal vez termine desajustada de las dimensiones o las dosis de las sanciones penales de otro tipo de conductas que tal vez no sean tan coyunturalmente trascendentes, pero que desde el punto de vista de la recriminabilidad social son iguales o peores. Entonces, no digo que comparto o que no comparto; sugiero mantener y defender conscientemente el grado de sanción que se propone y mirarlo en conjunto.

La diferencia del artículo 358 TER con el artículo 358 es que no se requiere la existencia de denuncia de parte. Solo a título de mera advertencia me voy a referir a lo que decía hoy el magíster Folgar con respecto al daño a la reputación. Imaginen ustedes un banco que deba admitir y hacer público que su seguridad -la seguridad informática de sus datos y demás- ha sido vulnerada. La corrida bancaria de esta institución en caso de llegar eso a conocimiento del público es mucho mayor, mucho más grave, y tiene consecuencias económicas muchísimo mayores que las de no decirlo, haber pagado el seguro, ir a cobrarlo cuando ocurre el siniestro y adoptar las medidas para evitar que eso suceda en el futuro, porque nadie lo va a hacer por gusto. Entonces, no estamos pidiendo denuncia de parte. Estamos asumiendo que el Estado, en caso de tomar conocimiento, va a analizar esta conducta, la va a sustanciar penalmente y, eventualmente, la va a castigar. Reitero: no digo que deba decirlo o que no deba decirlo. Pensemos que, tal vez, tengamos que dar algún grado de reserva especial a la investigación. La eliminación de la denominación o la individualización de la entidad o sujeto damnificado es algo para pensar.

Con respecto al artículo 5º tenemos también alguna diferencia, en la medida en que el artículo 297 castiga con pena pecuniaria, y en el inciso segundo estamos hablando de pena privativa de libertad. Simplemente quiero advertir que nos estamos apartando; de repente hay razones específicas vinculadas a la trascendencia de la conducta reprochable, pero hay que tener en cuenta que estamos modificándolo.

Si les parece de utilidad, les voy a pasar un informe por escrito para ordenar esto. Pido disculpas por no haberlo traído a la Comisión en el día de hoy; lo remitiré oportunamente si les parece de utilidad.

El artículo 6º agrega el inciso tercero, "Vulneración de Datos", que dice: "El que, por cualquier medio acceda, se apodere, utilice, o modifique datos reservados de terceros […]". Nosotros tenemos leyes que definen y califican, de acuerdo a su confidencialidad, a su reserva o a su secretismo, determinados datos. La Ley N° 18.331 refiere y define lo que son datos personales, datos sensibles y datos especialmente protegidos; es la que nos habla de la reserva, de la confidencialidad. Cuando hablamos de datos reservados, ¿estamos refiriéndonos a alguna de estas categorías? No sé si cuando hablamos de datos reservados no sería más conveniente referirnos -si esa es la voluntad- a algunas de las categorías que la Ley Nº 18.331 nos define, que al fin y al cabo es parte del ordenamiento y es norma. Es decir, personal, sensible o especialmente protegido, o todos ellos. No lo digo yo, lo definirán ustedes.

En el artículo 7º, "Suplantación de identidad", se sugiere -sobre todo por la gente que sabe del tema- la inclusión de las plataformas digitales en general porque, si no, podría interpretarse que las plataformas digitales educativas estarían quedando fuera de las previsiones del inciso 3º del artículo 347. Voy a decir algo, y es probable que se enojen conmigo, pero hay algunos verbos que están conjugados en modo subjuntivo y otros en indicativo. Perdón, pero es deformación profesional. Se usa uno u otro. En general, el Código Penal lo expresa en modo subjuntivo; quizá sea mejor.

El inciso 3 del artículo 347, establece: "El que usurpe, adopte, creare o se apropie de la identidad de otra persona física o jurídica, valiéndose de cualquier medio, herramienta tecnológica o sistema informático; […]". En realidad, sería conveniente incluir las plataformas digitales en general. Así, quedarían definidas o incorporadas las plataformas digitales educativas.

SEÑOR FOLGAR (Leandro).- Sugerimos incluir las plataformas digitales en general, de manera que queden también comprendidas las educativas.

SEÑOR GIANERO (Gastón).- La otra parte, refiere al modo de conjugación de los verbos: "El que usurpare, adoptare, creare o se apropiare […]".

El inciso 3. del artículo 347, podría decir: "El que usurpare, adoptare, creare o se apropiare, valiéndose de cualquier medio, herramienta tecnológica o sistema informático; obteniendo datos, accediendo a redes sociales, casillas de correo electrónico, cuentas bancarias, plataformas digitales asociadas a medios de pago, o cualquier credencial digital o factor de autenticación, […]". Pero ¿qué es esta enumeración? ¿Por qué necesitamos esta enumeración? ¿No estaremos complicándonos por dejar fuera otras? "El que" -perfecto, sujeto activo- "usurpare, adoptare, creare o se apropiare" de la identidad, claramente, sería la conjugación del verbo típico. Continúa: "[…] valiéndose de cualquier medio, herramienta tecnológica o sistema informático;". Bien, sería una condición objetiva. Sigue: "[…] obteniendo datos, accediendo a redes sociales, […]". ¿Es lo que se obtiene valiéndose de cualquier medio? No sé. Hay algo en la redacción que me complica. Si yo tengo que solicitar, además de que se valga de cualquier medio, que esté "obteniendo datos" ¿es acumulativo o alternativo? Tal vez sea incapacidad mía, pero se me complica la lectura y la comprensión de lo que estoy hablando cuando digo "obteniendo datos, accediendo a redes sociales, casillas de correo electrónico". ¿Son ejemplos?

(Diálogos)

—— ¿Cuál es la conducta sancionable? La conducta sancionable es la de aquel que usurpe, adopte, cree o se apropie de la identidad de otra persona física o jurídica, y que ello lo cometa valiéndose de cualquier medio, herramienta tecnológica o sistema informático. Obtenga o no obtenga datos, si usurpó la identidad de otra persona, usurpó la identidad de otra persona e incurrió en la conducta penalmente reprochable. ¿O tal vez me quiera decir el texto que la forma de usurpar, además de ser por medios tecnológicos, es obteniendo datos? Tengo que exigir eso. Cuando un juez vaya a aplicar esto, dirá: "Es cierto. Usted se apropió de la identidad de otra persona". Pero, en realidad, no obtuvo dato ninguno de la otra persona, o sí los obtuvo porque, si no, no se hubiera podido apropiar. No sé si es un supuesto de la apropiación de la identidad de una persona o una conducta adicional a desarrollar con la sustitución o adopción de la identidad de otra persona. Esta sería la consulta a los efectos aclaratorios. Técnicamente, el texto puede estar perfecto pero, cuando se vaya a aplicar por parte del Poder Judicial, los abogados lo podremos interpretar de una forma o de otra. Al final, terminará desnaturalizándose.

SEÑOR FOLGAR (Leandro).- La sugerencia podría ser que se hablara de identidad digital, por ejemplo, y que ello estuviese definido adecuadamente.

(Se suspende la toma de la versión taquigráfica)

SEÑOR GIANERO (Gastón).- Sugerimos la siguiente redacción: "El que usurpare, adoptare, creare o se apropiare de la identidad digital de otra persona física o jurídica, valiéndose de cualquier medio, herramienta tecnológica o sistema informático; con o sin la intención de dañar a su legítimo titular, será castigado con un año de prisión a seis años de penitenciaría".

No sería serio legislar en el momento porque ustedes tienen estudiado el tema más que yo. Sin embargo, la pregunta es la siguiente: si el obtener datos, el acceder a redes sociales es el uso que se hace de esa identidad o es la forma en que se apropia de la identidad digital. Esto no es lo que yo sostengo, sino lo que ustedes quieran plasmar.

El problema es el siguiente. Si yo me apropio de la identidad digital de cualquiera de ustedes ¿cuándo seré penado? ¿Cuándo me meta en sus redes sociales y hable por ustedes y diga cosas que afecten su reputación o su buen nombre? Si yo me apropio de la identidad de ustedes pero no la uso ¿incurro en inconducta o no? ¿O me está castigando el haber utilizado datos personales para apropiarme de la identidad? Eso debería aclararse. Si la norma va a exigir la obtención de datos, el acceso a las redes sociales y a las casillas de correo electrónico, habría que pensar si el que hizo todo el esfuerzo para adoptar la identidad digital de otra persona y fue interrumpido en su intención de salir a hacer publicaciones ofensivas para quien las emite, por ejemplo, aprovechándose de la identidad de ustedes, puede ser penado. ¿Va a ser penado a título de tentativa? ¿Es parte del *iter criminis* o no? ¿O el delito solamente es la apropiación de la identidad digital, la use o no la use? ¿Y yo lo hice por bueno, por malo o por hablar bien de ustedes? Eso hay que definirlo.

Con respecto al artículo 10°, que refiere a la campaña nacional educativa, es muy necesaria e importante la previsión. Tendríamos algunas apreciaciones para formular.

SEÑOR FOLGAR (Leandro).- En el Capítulo II sobre las medidas educativas, en el entendido de que estas competencias para el uso seguro y responsable que presentamos más temprano están establecidas dentro de un acuerdo entre el Ministerio de Educación y Cultura, ANEP y Agesic, que Ceibal está también promoviendo, sería interesante que pudieran estar incluidos dentro del listado de acciones y medidas que está descrito a continuación. Dice que los conceptos a desarrollar serán los siguientes y hay una lista descriptiva. Sería bueno incluir: "consideramos adecuado agregar los conceptos

descriptos en la presentación con respecto seguridad". Los conceptos son: autorregulación, comportamiento ético, comportamiento empático, conocer y ejercer los derechos en el entorno digital. Las competencias están en la presentación que vamos a dejar a la comisión.

SEÑOR PRESIDENTE.- Agradecemos mucho por la información. No hay nada por lo que tengan que disculparse; justamente los invitamos para esto, para que nos aporten su visión.

SEÑOR REPRESENTANTE CAL (Sebastián).- Agradecemos a la delegación por los aportes.

Nosotros realmente entendemos, por lo menos yo, que la parte que más les competía a ustedes era la campaña nacional de educación, pero igual son muy bien recibidos los demás aportes que realizaba el doctor Gianero. Hay algunos puntos específicos sobre los que quisiera preguntar. Hay un tema que se ha repetido en más de una oportunidad, y es que a algunos juristas no les ha gustado mucho el manejo de la terminología en inglés, como muy bien decía el doctor Gianero. A modo de aporte, he planteado la misma pregunta a todos, y es la siguiente: ¿qué nombre le daría al *grooming*? Ahí seríamos nosotros los que quedaríamos en desigualdad con el resto del mundo, porque en China se llama *grooming*, en Francia se llama *grooming*, en Italia se llama *grooming* y en Estados Unidos se llama *grooming*. Y la terminología que maneja el convenio de Budapest, es *grooming* para todos los países.

Sin duda que la cooperación internacional es una pata indispensable para esto; nosotros no la desconocemos y estamos trabajando en la adhesión al convenio de Budapest. Son muchísimos los países que están adheridos al convenio de Budapest, como muy bien decía el doctor Gianero, y hay muchos que están corriéndola de atrás, como Uruguay, en materia de ciberseguridad. Creo que este proyecto de ley sobre tipificación de ciberdelito se está convirtiendo en un proyecto mucho más amplio de ciberseguridad. De hecho, creo que el punto más importante de esta iniciativa es la campaña nacional de educación, que seguramente se va a convertir en una política de Estado que va a perdurar por varios años. Difícilmente podrá tener incrementos, pero no creo que alguien la quite porque va a ser parte indispensable del mundo por venir y del mundo de hoy.

En conclusión: me gustaría saber si ustedes tienen alguna sugerencia con respecto a la terminología en inglés porque, hasta ahora, hemos recibido el mismo comentario en repetidas oportunidades en cuanto a que puede no ser muy cómodo manejar alguna terminología en inglés en el Código Penal. Si bien pensamos poner alguna aclaración del significado de la palabra *grooming,* hasta ahora no me han dado, por lo menos a mí, ningún término que pueda ser claro para con las adhesiones internacionales que necesitamos en el combate a la ciberdelincuencia. Podrá no ser lo habitual, lo que más guste, pero entendemos que el Código Penal tendrá que adaptarse a acuerdos de cooperación internacional como el convenio de Budapest, que es tan importante para el combate a la ciberdelincuencia.

¿Por qué digo que este no es solamente un proyecto de tipificación penal? Primero, porque ya tiene una campaña nacional de educación que creo que va a ser base indispensable para convertirnos en una sociedad más blindada en temas de ciberseguridad, y segundo, porque tenemos alguna propuesta que seguramente haremos cuando empecemos el tratamiento del proyecto de ley, que hemos estamos compartiendo con los demás legisladores de esta comisión, como por ejemplo la creación de un registro nacional de ciberdelincuentes.

Yéndome del tema educativo, que era el que principalmente pensaba comentarles, quiero señalar que hoy la modalidad de mulas de dinero es indispensable para la operativa de muchos delitos que se están cometiendo. Hoy, una persona que tiene una cuenta bancaria en determinado banco realiza transacciones; cuando se detecta que la persona está usando la cuenta bancaria con ese fin, se le cierra, pero va y abre una cuenta en otro banco sin ningún tipo de perjuicio. Entonces, creo que también es importante generar un registro nacional de ciberdelincuentes para tratar de limitar estas modalidades de mulas de dinero. Entonces, esta iniciativa excede un poco más de lo que es la mera tipificación del ciberdelito.

También tenemos para analizar una propuesta del Banco Central muy interesante para tratar de dar a la banca privada una herramienta que bloquee los fondos de manera más veloz. El otro día el Banco Central nos decía que a veces demoran aproximadamente unas dos semanas en dar una orden para bloquear fondos, y eso es tremendamente impráctico e ineficiente para una transferencia bancaria. Hoy, con la banca digital, las cosas tienen que ser más rápidas. Ese un punto que tendremos que analizar. Como ya dije, este es un proyecto de ley mucho más amplio que si fuera solamente tipificar los delitos. De todas formas, fueron muy bien recibidos los aportes y de mi parte los voy a estar revisando. Lo que más me interesa es la terminología y ver qué idea o sugerencia tienen al respecto para que nos puedan entender los franceses, los chinos y los norcoreanos, porque esto es un ida y vuelta con Budapest. No es que yo me sumo a Budapest y solamente recibo beneficios; también los tengo que brindar. Entonces, es muy importante para mí saber eso.

SEÑOR REPRESENTANTE LORENZONI HERRERA (Miguel).- Quiero agradecer al doctor Gastón Gianero y al magíster Leandro Folgar por las exposiciones que hicieron; fueron muy claras.

Quiero hacer algunas preguntas sobre el Capítulo II, que refiere a las medidas educativas. Folgar hacía referencia al concepto de ciudadanía digital y al grupo de trabajo de ciudadanía digital. Quisiera saber qué posibles contribuciones ven que puede hacer el grupo de trabajo de ciudadanía digital que integran el Ministerio de Educación y Cultura, el Plan Ceibal y otras dos entidades más para la campaña nacional educativa prevista, justamente, en el Capítulo II, y en particular si esto se amolda a la estrategia de ciudadanía digital de la que esbozaba algunos conceptos el magíster Folgar. Por otra parte, también vinculado a la creación de la Campaña Nacional Educativa, quisiera saber si actualmente el Plan Ceibal está llevando adelante algún tipo de acción concreta en cuanto a la promoción y concientización de la ciberseguridad y, en particular a la cuestión del manejo de las finanzas en los entornos personales; si se están haciendo cursos en ese sentido. Me gustaría saber si existe la capacidad para poder llegar a cubrir a la población objetivo que establece el proyecto de ley, es decir, a los estudiantes de Secundaria, escuelas técnicas -también comprendidas- y a los beneficiarios de las prestaciones servidas por el Banco de Previsión Social e Inefop.

Quisiera hacer una pregunta a ambas delegaciones. ¿Cómo creen que puedan contribuir tanto el MEC como el Plan Ceibal en la capacitación de personal para dictar los cursos contemplados en el proyecto? ¿Existen posibilidades, eventualmente, luego de ampliar el universo de población destinataria, más allá de lo que establece el proyecto?

También tengo dos preguntas, una para el Ministerio de Educación y Cultura y otra para el Plan Ceibal.

En cuanto al MEC, sobre el capital humano, ¿quiénes consideran que son las personas más idóneas para poder orientar y dictar este tipo de cursos?

Por otra parte, ¿cuáles son los medios por los cuales les parece más adecuado que este tipo de actividades o este tipo de capacitaciones se lleven adelante dentro de los centros educativos públicos de nuestro país y de qué manera podrían llevarse a cabo durante un año lectivo normal?

Para el magíster Folgar: ¿cree que este tipo de iniciativas -y esto que esbozaba también en la diapositivas- puede desarrollarse plenamente a través de lo que son las plataformas y las modalidades virtuales y, en particular, se pueden hacer a través de lo que dispone el Plan Ceibal?

SEÑOR FOLGAR (Leandro).- Muchas gracias por la atención con la que nos han escuchado y por las preguntas, que creo que son sumamente importantes.

En cuanto a qué acciones se están tomando en concreto, esto de poder alinear la estrategia de ciudadanía digital como una estrategia paraguas que esté en toda la propuesta educativa, tanto de la ANEP como de Ceibal, es la primera, y eso se vuelca en forma de cursos específicos que están tomando los estudiantes en todos los niveles y que están dentro del área de formación de Ceibal, disponibles para docentes y para que después derramen con los estudiantes.

Sí existe una dificultad que siempre está en el sistema educativo, que tiene que ver con el espacio curricular destinado a esto. Ceibal, en sus plataformas, puede destinar los cursos, los diseños, pero siempre es la mediación de los adultos la que genera que estos cursos y contenidos sucedan en consonancia con el tiempo de los estudiantes. Entonces, tendrá que haber también en el rediseño curricular o dentro de las propuestas extracurriculares un espacio destinado para tal fin. Eso es algo que Ceibal no controla unilateralmente dentro de lo que es la educación formal. Si hubiera programas adicionales extracurriculares que otras organizaciones decidieran llevar adelante, los contenidos y los cursos podrían estar dentro de las plataformas de Ceibal y el Plan Ceibal, encantado, los podría poner al servicio.

Con respecto a iniciativas concretas -por ejemplo, hoy se comentó una específica del Banco Central- puedo decir que hemos tenido una aproximación de parte del Banco Central, porque ellos tienen una estrategia de formación que está disponible dentro de las plataformas de Ceibal, pero -de nuevo- todo depende de cuánto contenido los docentes vayan decidiendo incorporar.

Por otra parte, lo que sí tiene Ceibal es una estrategia de formación en el uso adecuado de las tecnologías y en el ejercicio de la ciudadanía en ámbitos digitales. Es una estrategia concreta, en la que está trabajando con Unicef, con Unesco y con otros socios, que se materializa en programas que pueden ser virtuales, pero también presenciales.

El aporte que se puede hacer del grupo de trabajo en conjunto tiene que ver con alinear las estrategias de ciudadanía digital e, incluso, el concepto de ciudadanía digital para que fomente la adquisición de estas competencias que hoy presentaba, que tienen que ver con la autorregulación, el comportamiento ético, el comportamiento empático y conocer y ejercer los derechos en el entorno digital. Ahí vamos a necesitar, sin duda, muchas colaboraciones y asistencia.

En cuanto a la conciencia de la huella digital cabe destacar que hoy se habló largo y tendido sobre la identidad digital y demás y cómo esa identidad o el trazo de lo que hacemos en las redes queda estable allí, en lo que tiene que ver con el manejo de la privacidad y el manejo de los riesgos. En todas esas competencias Ceibal está tomando acciones educativas concretas en conjunto con la ANEP y con algunos otros socios externos. El Banco Central es uno de los organismos con los que hemos estado en

contacto. También tenemos toda la línea de educación social y cívica, que también está mirando este tema.

Creo que respondí todas las preguntas.

Gracias.

SEÑOR GIANERO (Gastón).- En primer lugar -no hubo recriminación al respecto-, pido disculpas por haberme metido en temas estrictamente jurídicos, pero es muy difícil hablar con un abogado sobre un proyecto de ley y que no intervenga ni opine en materia jurídica. Si puede colaborar y aportar, fantástico. Si no, pido disculpas por el tiempo perdido.

Con respecto al tema de la Campaña, cabe decir que la Dirección de Educación, con el área de educación no formal, en coordinación con ANEP, va a ser la que tome a su cargo, en lo que corresponde -por supuesto, en combinación con el Plan Ceibal-, el aporte de recursos humanos. Creo que, además, se va a involucrar en la Campaña a muchos otros organismos -eventualmente, instituciones bancarias y demás- que también, de alguna forma, deben facilitar y difundir la protección, el cuidado y el manejo responsable de esas herramientas informáticas. Con lo cual sería a través de la Dirección de Educación -área de educación no formal- que se dispondría el cumplimiento de la norma una vez que se disponga que se inicie, sin perjuicio de que, como decía el magíster Folgar, desde el Plan Ceibal se vienen desarrollando acciones concretas al respecto.

Tomando el planteo que hacía el señor diputado Cal con respecto al neologismo, no descarto que lo que señalé respecto al neologismo sea de antiguo o de tradicionalista. No lo descarto. Sí descarto el tema de la soberanía de la lengua.

Lo que me preocupa como juzgado es que la utilización del término extranjero habilita a que un tercero, un colectivo ajeno a nuestro ordenamiento jurídico, sea el que le dé contenido al tipo penal. El hecho de designarlo con nuestra terminología y con nuestros propios términos, en nuestro idioma, nos da un control sobre la interpretación y el contenido que tiene esa figura delictiva.

Con respecto a la inserción en el mundo, nos pasa con *grooming* o con *stalking* y con cualquier otro término que en materia de cooperación jurídica internacional sea un delito respecto del que intervengan más de una jurisdicción con más de un idioma. No sé si es el mejor, pero el propio texto proyectado incluye alternativas a *stalking* o a *grooming*. *Stalking* o acoso telemático; *grooming* o acercamiento físico o virtual. Insisto: es el *nomen iuris*, no es el que define la conducta. Esto sirve como argumento para decir: "Bueno, y entonces ¿qué tanto molesta que sea extranjero, que sea un neologismo o no?". Está bien. Insisto: tal vez es un tema generacional. El ordenamiento jurídico debe expresarse en nuestro idioma porque al fin y al cabo es nuestro idioma el que le brinda las herramientas de interpretación de su contenido. No resultaría conveniente que yo abriera las puertas para que un juez, al momento de aplicar una norma nacional, tomara parte del contenido que a un término en otro idioma se da en otro país o en el idioma nativo de ese término. Lo único que me dejó tranquilo es que hay otros colegas que han opinado igual. No sé si tengo razón, pero hay otros antiguos como yo. No sé si es un tema de generación.

Lo que me preocupa es la regla de interpretación; lo dice el propio texto. Si el inciso segundo del artículo 288 proyectado dice "acoso telemático" como *nomen iuris,* dejemos "acoso telemático". Si "acoso telemático" no representa el nombre que le queremos dar a la conducta, busquemos otro. Pero tampoco pongámoslo como denominación alternativa.

¿*Stalking* o acoso telemático? Me pueden decir: "Bueno, doctor Gianero usted me genera el problema porque me dice que no le gusta *stalking*. ¿Cuál le gusta o cuál le parece a usted que refleja mejor?". Entonces -no lo haría- yo le diría: "Bueno, pero ustedes mismos dijeron que "acoso telemático" es la forma de expresarlo". Entonces, ¿qué me aporta *stalking* si tengo "acoso telemático"? O de lo contrario, si "acoso telemático" no refleja el concepto de *stalking*, entonces tal vez deberíamos retirar "acoso telemático". Es decir, ya está la alternativa. No digo que esté bien o no. El redactor o redactores del proyecto entendieron que "acoso telemático" era sinónimo suficientemente fidedigno, por lo menos para el *nomen iuris,* de *stalking.* Y entendieron que "acercamiento físico o virtual" era lo suficientemente descriptivo o comprensivo de *grooming*.

¡A ver! En este punto mi intervención es absolutamente indebida en la medida de que los legisladores son ustedes. Simplemente, por deformación profesional, uno se para frente a un texto legal y no se puede resistir a hacer apreciaciones de índole legal. Perdón.

SEÑOR REPRESENTANTE LORENZONI (Miguel).- Muchas gracias por las respuestas.

Me queda una consulta pequeña y breve.

El Plan Ceibal maneja un concepto de ciudadanía digital. ¿Ese concepto lo ha tomado el grupo de trabajo de ciudadanía digital como propio para la elaboración de todo lo que es la estrategia de ciudadanía digital en conjunto? Porque me parece que el grupo en su totalidad tiene un potencial enorme y quiero saber si ya se está trabajando en forma articulada para avanzar eventualmente en este terreno.

SEÑOR REPRESENTANTE MENÉNDEZ (Rafael).- Buenos días.

Sobre todo me quedé preocupado por la argumentación de uno de los artículos en el entendido de cómo está preparado Uruguay o cómo va encarar, vista la extraterritorialidad de este tipo de delitos, las penas y su aplicación. Francamente no entiendo cómo se puede tipificar de manera práctica un delito de estos a un ciberdelincuente instalado en Asia. ¿Cuál va a ser la respuesta? ¿Cómo está preparado nuestro país para dar respuesta a este tipo de delitos?

SEÑOR REPRESENTANTE MELAZZI (Martín).- Se habló de la identidad digital -justamente el artículo 347 habla de identidad-, ¿la definición de identidad digital se encuentra en algún lado como para tipificar este tipo de delitos llegado el momento? ¿Está dada la definición de identidad digital?

SEÑOR FOLGAR (Leandro).- Se ha discutido respecto a si se maneja una definición de manera conjunta; se mantiene una comisión permanente de diálogo a la que se integra el esfuerzo de transformación digital en torno al liderazgo de la Agencia del Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Lo que sí es importante y hemos procurado hacer, es que desde la perspectiva educativa, el concepto de ciudadanía digital esté compartido por la ANEP y por Ceibal, fundamentalmente, ya que nuestro cometido es con el sistema educativo formal de tres a dieciocho años de edad, sector al que fundamentalmente brindamos servicios. Eso no quita -es una buena pregunta que se trajo recién- que tengamos un espacio de diálogo para *agiornar* permanentemente el concepto de ciudadanía digital entendiendo que está muy asociado a las tecnologías digitales y que estas evolucionan de manera muy rápida.

Y con respecto al concepto de identidad digital desde mi desconocimiento absoluto desde el punto de vista jurídico, sí entiendo que es un concepto que viene ganando tracción y que se utiliza -incluso tenemos agencias de gobierno que nos brindan una identidad digital- ; deberíamos tener esa definición por lo menos para el país.

Entonces, respecto a agregar el concepto de identidad digital, dado que ya tenemos agencias de gobierno que lo están utilizando, sería prudente tenerlo definido y que pueda ser utilizado en las legislaciones.

SEÑOR GIANERO (Gastón).- Comienzo por esto último.

No conozco norma legal que recoja, defina o determine el concepto de identidad digital, más allá de que parecería que pudiéramos decirlo. Es cierto y adecuado que eventualmente el propio proyecto contenga una definición de qué se entiende por identidad digital, porque claramente tiene un contenido distinto al de identidad. Hay muchísimas conductas que podrían suponer la suplantación de la identidad digital y que absolutamente de ninguna forma supondrían suplantación de la identidad. No es imaginable, salvo que me disfrace -por lo menos en el concepto tradicional-, que pueda suplantar la identidad de otra persona. Sí estamos hablando de identidad digital y estaría muy bien que se incluyera una definición.

Con respecto al planteo del señor diputado Menéndez, efectivamente la jurisdicción es la parte que requiere mayor análisis del Convenio de Budapest. Es decir, cómo hacer para castigar efectivamente el ciberdelito o para hacer efectiva la represión penal del ciberdelito. Como jurisdicción, el Convenio de Budapest establece pautas a adecuar y a adoptar por normas nacionales de cada uno de los Estados, pero la sugerencia o la intención de Budapest es que se pueda adoptar jurisdicción o se haga competente la jurisdicción nacional, cuando el delito se haya cometido en el territorio del país -no cabe ninguna duda, es el régimen general-, a bordo de un buque que enarbole su pabellón o a bordo de una aeronave matriculada. Está bien, son los casos de reputación del territorio nacional, y agrega: "[…] por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió […]". Esto supone una especie de portación del ordenamiento jurídico en la mochila de cada nacional que ande por el mundo. Es novedoso y es adecuado, fundamentalmente, en la medida que exige que el tipo delictivo también esté previsto como tal en el país en el cual se comete. De lo contrario, cabría la posibilidad de que uno terminara siendo responsabilizado penalmente de una conducta que no es penalmente punible, solo por ser nacional de un Estado que, eventualmente, hace cuarenta años no visita; no lo sé. Esta es una buena medida.

El Convenio también señala: "[…] o si ningún Estado tiene competencia territorial respecto de mismo". Esto tiene manifestación espejo en lo que es el proceso de extradición y el proceso de cooperación jurídica internacional. Es decir, las reglas de la cooperación jurídica internacional y los tratados, los convenios o la legislación -se está estudiando el proyecto de ley nacional de cooperación internacional- definen las medidas, los mecanismos y las formas de hacer efectiva la cooperación jurídica internacional. Además -me resisto a decir que la pandemia trajo algo bueno y no lo trajo-, se ha desarrollado la vía digital o el medio digital como una herramienta indispensable para hacer efectiva la cooperación jurídica internacional; forzado, pero se ha instalado.

Por medio de los instrumentos de cooperación jurídica internacional, se haría posible la represión y la aplicación efectiva de la pena respecto a los delitos previstos.

Muchas gracias.

SEÑOR PRESIDENTE.- Muchísimas gracias. Agradecemos los aportes al doctor Gastón Gianero y al magíster Leonardo Folgar, que serán considerados por la Comisión.

Informo a los integrantes de la Comisión que el Banco Central remitió una información en relación a una nota de prensa que fue publicada bajo el título: "Aumentó el 25 por ciento el ciberdelito en los dos últimos dos años". El material ya nos llegó y será distribuido a los miembros de la Comisión.

No habiendo más asuntos, se levanta la reunión.

